REMARKS

No claims have been amended or canceled. Claims 1-13, 15-20, and 22-24 remain pending in the case. Further examination and reconsideration of pending claims 1-13, 15-20, and 22-24 are respectfully requested.

Section 103 Rejections

Claims 1-3, 8-13, 15-20, and 22-24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,047,067 to Rosen (hereinafter "Rosen") in view of Applied Cryptography by Schneier (hereinafter "Schneier"). In addition, claims 4-7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Rosen in view of Schneier and further in view of U.S. Patent Application 09/751,856 to Harif (hereinafter "Harif"). Applicant respectfully traverses this rejection in its entirety and incorporate by reference the arguments made in the previous Response to Office Action Mailed April 11, 2003 (hereinafter "Previous Response").

In order to sustain the Examiner's burden of showing a *prima facie* obviousness of a claimed invention, three essential criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. Second, there must be a reasonable expectation of success. As stated in MPEP 2143.01, the fact that references can be hypothetically combined or modified is not sufficient to establish a *prima facie* case of obviousness. *See In re Mills*, 916 F.2d. 680 (Fed Cir. 1990). Finally, the prior art references must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d. 981 (CCPA 1974); MPEP 2143.03, emphasis added. Specifically, "all words in a claim must be considered when judging the patentability of that claim against the prior art." *In re Wilson* 424 F.2d. 1382 (CCPA 1970). Using these standards, Applicant asserts that the cited art fails to teach or suggest all features of the currently pending claims. In addition, the cited art cannot be combined according to the hypothetical creation set forth in the Office Action since to do so would destroy the intended purpose of the references which explicitly teach away from that which is presently claimed. Some distinctive features of the present claims are set forth below.

Rosen and Schneier do not teach, suggest, or provide motivation for maintaining the identities of the network members (i.e., network client, network host, or both) confidential to only the financial resolution unit. Present claim 1 states in the last element that the identity of the network

client and network host are known only to the financial resolution center (FRC). Likewise, claims 15 and 20 recite confidentiality in general; claims 19-23 note confidentiality of a computational device found within a host or client. In all instances, however, each of the independent claims describe the importance of maintaining the identity of the network client and network host confidential, and unknown to the other -- i.e., unknown to any of the computational devices or network members coupled to the network. The present specification defines the network members as the network client, network host, and intermediary network server (Specification -- Fig. 1).

As argued in the Previous Response, Rosen requires the bank issuing the electronic credit or currency to be known and sent along with the information to the recipient in order to "preserve the integrity of the electronic monetary system." (Rosen -- col. 4, lines 4-9.) There are many examples provided by Rosen; however, each example specifically requires that the identities of at least one party (and often both) involved in a transaction are disclosed (Rosen – col. 16, lines 53-54; col. 19, line 45; col. 24, lines 48-55; col. 26, lines 58-61; col. 3, lines 23-30). The purpose behind disclosing the identity of the payer or payee and the arguments as to why this disclosure would teach away from at least one feature of the currently pending independent claims are set forth in pages 9-13 of the Previous Response.

Apparently, the Office Action agrees with the arguments made in the Previous Response and states that "Rosen ('067) does not explicitly disclose identities of the network members are known only to the financial resolution center." (Office Action -- page 3 when discussing claim 1, and page 4 when discussing claim 15.) Moreover, the Office Action notes that Rosen does not explicitly disclose a network client that remains unknown to a computational device or the general maintaining of confidentiality as to the identity of the network client and the network host (Office Action – page 5 when discussing claims 19 and 20.) While Applicant would agree in part with the characterizations made in the Office Action, Applicant must disagree that Rosen simply does not "explicitly disclose." Instead, Applicant asserts that Rosen explicitly "teaches away" from the present claims. As such, Applicant also contends that Rosen cannot be used as demonstration of *prima facie* obviousness. Indeed, according to the Federal Circuit, teaching away is the antithesis of obviousness and is *per se* demonstration of lack of *prima facie* obviousness. *In re Dow Chemical Co.*, 837 F.2d 469 (Fed. Cir. 1988); *See also In re Hedges*, 783 F.2d. 1038 (Fed. Cir. 1986); MPEP 2143.03.

Thus, when looking in the financial industry and, upon examining Rosen, a person skilled in the art would certainly not be led to believe that maintaining the secrecy of the identities of the network members is obvious. More importantly, a person skilled in the art would not look to Schneier to form that nexus. Upon a close examination of Schneier, it discloses essentially that which is described in the "Background of the Invention" section of the present specification. Schneier illustrates the importance of encryption using what is known as "public-key cryptography." The same cryptography using public-key encryption is described in the Background section of the present specification, pages 4-5. An essential requirement of public-key cryptography using two keys (i.e., a public key and a private/session key) is that the recipient of a message must send his public key to the sender, and the sender must thereafter use that public key when encrypting the message. While encrypting the message, the sender will also place an encrypted private (or session) key into the message so that the recipient can then decrypt the session key and the underlying message using his private key and session key.

Public-key cryptography relies on the exchange of keys and, more specifically, the recipient knowing the identity of a potential sender so that the recipient will forward his public key to the sender. In return, the sender must know the identity of a recipient so that the sender can send his private key and/or session key to the recipient in order to decrypt the message. Even still, once the decryption has occurred, obviously the recipient will know who sent the underlying, decrypted message.

The Office Action appears to interpret page 51 of Schneier as somehow avoiding the public key handshaking mechanism, where keys are exchanged between a known sender and recipient -- i.e., by the recipient somehow knowing the sender and the sender somehow knowing the recipient. On page 51 of Schneier, the subheading "Key and Message Broadcast" is clearly referring to the broadcast of a message. However, before the sender (Alice) can broadcast a message to multiple recipients, Alice must know which recipients among those broadcasted recipients are to receive the message – Bob, Carol, and Dave are the only recipients who will be able to decrypt the message. Sender (Alice) does this by obtaining Bob's, Carol's, and Dave's public keys from Alice's database and, thereafter, encrypts the message with those public keys. Again, Alice must know the identity of Bob, Carol, and Dave as the recipient before Alice can search the database for the appropriate public keys. Once encrypted with Bob's, Carol's, and Dave's public keys, the message is broadcast to multiple recipients, but only Bob, Carol, and Dave can decrypt using their respective private keys. Thus, while the message is broadcast, the recipients (Bob, Carol, and Dave) must be known to the sender in order for the sender (Alice) to search her database for their public keys.

The example described in Schneier makes clear that the sender must know the identity of the recipient in order to ensure the recipient can properly decrypt the encrypted message. The sender does this by placing the unique public key for the recipient into the message. Similar to Rosen, Schneier appears to teach away from the present claims which maintain the identity of the network members confidential -- i.e., the network host (sender) does not know the identity of the network client (recipient) or vice-versa. To somehow infer that the sender in Schneier not know the identity of the recipient would defeat the entire purpose of public-key cryptography described therein.

For at least the reasons set forth above, independent claims 1, 15, 19, 20, and 23, as well as claims dependent therefrom, are asserted to be patentable over Rosen and Schneier, either individually or in combination. Accordingly, removal of this rejection is respectfully requested.

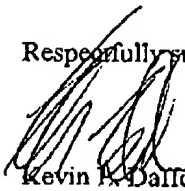
In addition, several of the dependent claims are believed to be separately patentable. For example, claim 2 recites in part: ". . . wherein the network members are determined by the financial resolution center." This feature in combination with the features of independent claim 1 do not appear to be taught or suggested by the prior art.

CONCLUSION

This response constitutes a complete response to all issues raised in the Office Action mailed October 23, 2003. In view of the remarks traversing the rejections presented therein, Applicants assert that pending claims 1-13, 15-20, and 22-24 are in condition for allowance. If the Examiner has any questions, comments, or suggestions, the undersigned attorney earnestly requests a telephone conference.

No fees are required for filing this amendment; however, the Commissioner is authorized to charge any additional fees which may be required, or credit any overpayment, to Conley Rose, P.C. Deposit Account No. 03-2769/5468-06500.

Respectfully submitted,



Kevin B. Daller
Reg. No. 34,146
Attorney for Applicant(s)

Conley Rose, P.C.
P.O. Box 684908
Austin, TX 78768-4908
Ph: (512) 476-1400
Date: January 22, 2004